UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,224	02/26/2004	Burkhard Kuhls	080437.53236US	2832

23911 7590 10/27/2008

CROWELL & MORING LLP
INTELLECTUAL PROPERTY GROUP
P.O. BOX 14300
WASHINGTON, DC 20044-4300

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,224	KUHLS, BURKHARD	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to application amendments filed on 7-25-2008.

2. Claims **1, 3 - 20** are pending. Claims **1, 5, 7, 8, 10, 11** have been amended. Claim **2** has been cancelled. Claims **1, 7, 19** are independent. The application was filed on 2-26-2004.

Response to Arguments

3. Applicant's arguments filed 7/25/2008 have been fully considered but they were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, specification objection. (see Remarks Page 8)

The specification objection has been withdrawn.

3.2 Applicant argues that the referenced prior art does not disclose, 112 rejection. (see Remarks Page 8)

The 112 rejection is maintained due to the non-disclosure of a generic “third” key or “third" signature in the specification or the original claims. See the 112 rejection.

3.3 Applicant argues that the referenced prior art does not disclose, “using the public key of the software signature site and a secret key of a control entity of a trust center”. (see Remarks Page 9, 10)

The England prior art discloses the manufacturer of a control unit. In addition, the manufacturer of the control unit is the software developer and stores the software into the control unit after manufacture of the control unit. (see Specification Page 1) The England prior art discloses a manufacturer's public/private key pair and a control unit's private or secret key. (see England col. 7, line 63 - col. 8, line 14: generates and issues a signed manufacturer (manufacture is also software developer) certificate; usage of public/private key pair; separate key pair (including a private or secret key) placed into a CPU (or control entity); signed certificate contains manufacturer's public key and the private (secret) key of the manufacturer's CPU (or control entity))

3.4 Applicant argues that the referenced prior art does not disclose, "England is not an analogous reference". (see Remarks Page 11)

The England prior art discloses a mechanism to protect content such as software. The software includes software developed for the operation of a control unit used in a vehicle. The content or software is protected using cryptographic techniques such as public/private key pairs and third party certificates.

The usage of a certificate mechanism as a security and access control mechanism is well known in the art. The usage of software to operate an entity such as a control unit that controls a vehicle is well known in the art. Computer controlled units for controlling the operation of a vehicle have been in use for quite some time. The usage of well known in the art techniques such as a digital signature has been used as a security mechanism for quite some time. Applicant's claimed invention appears to be a

large set of well known in the art certificates utilized as a security mechanism for a vehicle software system.

3.5 Applicant argues that the referenced prior art does not disclose, "checking by the control unit, whether the software signature certificate has been changed or manipulated". (see Remarks Page 12)

A better citation to disclose the determination of a certificate being compromised is the determination that a certificate has been placed on a certificate revocation list by the trusted third party. The England prior art discloses that a certificate has been revoked and placed onto the certificate revocation list. (see England col. 12, lines 27-30).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim **20** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. There is no disclosure of "a third public key and a third signature" within the specification or the original claims as amended in claim 20. This will be interpreted as a public key and a signature. Appropriate correction required. Applicant has amended the specification with information concerning a third key and signature. There is no previous disclosure of any indication of a generic "third" key or

"third" signature in the specification or the original claims. This is not a well known in the art feature and cannot be added to the specification without some basis for its addition. If Applicant feels there is a basis for its addition, please indicate the basis.

Claim Rejections – 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1, 3 - 20** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Wong et al.** (US Patent No. **5,957,985**) in view of **England et al.** (US Patent No. **6,330,670**).

Regarding Claim 1, Wong discloses:

a method comprising providing software for use by a control unit of a vehicle, (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software for vehicle control unit) Wong does not specifically disclose signing the software against falsification, using a secret or private key of a software signature site, and checking the signed software for integrity.

However, England discloses:

a) before its use by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; col. 11, lines

47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; sign boot code), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer signs software), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: private (secret) key of manufacturer's CPU (control entity)) and

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

England discloses that the boot code is signed (see England col. 8, lines 34-37; c0l. 11, lines 47-51: signed boot code). And, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate). This is equivalent to the specification on page 6, paragraph [0021], lines 3-6, which discloses that the software signature certificate is the generated and signed by the manufacturer of the software.

England discloses a digital certificate containing an identification number for a control entity (see England col. 8, lines 26-28; col. 9, lines 4-10: software identity; identify of an authenticated OS). This is equivalent to the specification on page 3, paragraph [0010] and paragraph [0012], which discloses that the clearing code

certificate contains an identifier and the capability to restrict usage to a particular control entity.

England discloses a trust center or a trusted third party for certificate signing. (see England col. 8, line 66 - col.9, line 3: trusted third party) This is equivalent to the specification on page 6, paragraph [0022], which discloses a trust center or trusted third party that generates certificates.

Wong does not specifically disclose generating a software signature certificate, using the public key of the software signature site and a secret key of a control entity. However, England discloses wherein generating a software signature certificate using the public key of the software signature site and a secret key of a control entity of a trust center, according to a public-key method. (see England col. 7, line 63 - col. 8, line 14: generates and issues a signed manufacturer (manufacture is also software developer) certificate; usage of public/private key pair; separate key pair (including a private or secret key) placed into a CPU (or control entity); signed certificate contains manufacturer's public key and the private (secret) key of the manufacturer's CPU (or control entity))

It would have been obvious to one of ordinary skill in the art to modify Wong to sign the software against falsification and check the signed software for integrity using a private key, and generation of a software signature certificate using the public key and a secret key of a control entity of a trust center as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of

England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61: *" ... Therefore, there is a need in the art for a digital rights management operating system that protects the rights of the content provider ... without requiring additional hardware directed at securing downloaded content. ... "*)

Regarding Claim 3, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: vehicle control unit) Wong does not specifically disclose a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. However, England discloses wherein one of a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity. (see England col. 7, line 63 - col. 8, line 14: manufacturer (CPU, control entity) certificate generated; manufacturer public/private key pair usage)

It would have been obvious to one of ordinary skill in the art to modify Wong for a control entity certificate and a trust center certificate to be generated according to a public-key method as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 4, Wong discloses the method according to claim 1. (see Wong col.

2, lines 21-29; col. 4, line 64 - col. 5, line 8: vehicle control unit) Wong does not specifically disclose clearing code data are signed using a secret key of a clearing code site according to a public key method. However, England discloses wherein clearing code data are signed using a secret key of a clearing code site according to a public key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer; col. 8, lines 7-12: public/private key pair usage)

It would have been obvious to one of ordinary skill in the art to modify Wong for clearing code data to be signed using a secret key of a clearing code site as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 5, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. However, England discloses wherein a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method. (see England col. 8, lines 26-37; col. 9, lines 4-10: software identify (clearing code site identifier); uniquely determines OS identity signed by manufacturer;

col. 8, lines 7-12: public/private key pair usage)

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, and checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 6, Wong discloses the method according to claim 3. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. However, England discloses wherein the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register; col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

It would have been obvious to one of ordinary skill in the art to modify Wong the trust center certificate is protected against falsification and exchange, in a protected memory area as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 7, Wong discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

a control unit of a vehicle. (see Wong col. 2, lines 21-29; col. 7, lines 32-38; col. 4, line 64 - col. 5, line 8: control unit for vehicle, control unit, boot image) Wong does not specifically disclose the clearing code site signature certificate, the software signature certificate, the clearing code data and their signature as well as the software and its signature are stored in the control unit.

However, England discloses:

a) before its use by the control unit, signing the software against falsification (see England col. 8, lines 34-37: boot block signed by OS manufacturer; col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; sign boot code), using a secret or private key of a software signature site (see England col. 8, line 66 - col. 9, line 2: software developer or manufacturer signs software), according to a public-key method; (see England col. 7, line 63 - col. 8, line 14: public key of manufacturer for CPU (control entity)) and

b) checking the signed software for integrity, using a public key complementary to the secret key of the software signature site, (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) wherein a clearing code site signature certificate, a software signature certificate,

the clearing code data and their signature as well as the software and its signature are stored in the control unit (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU; certificate contains public key), and the software signature certificate is generated using the public key of the software signature site and a secret key of a control unit of a trust center. (see England col. 7, line 63 - col. 8, line 14: generates and issues a signed manufacturer (manufacture is also software developer) certificate; usage of public/private key pair; separate key pair (including a private or secret key) placed into a CPU (or control entity); signed certificate contains manufacturer's public key and the private (secret) key of the manufacturer's CPU (or control entity))

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, checking the signed software for integrity, and the generation of a software signature certificate using the public key and a secret key of a control entity of a trust center as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 8, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not

specifically disclose software signature certificate includes at least one validity restriction. However, England discloses wherein the software signature certificate includes at least one validity restriction. (see England col. 8, lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

It would have been obvious to one of ordinary skill in the art to modify Wong that the software signature certificate includes at least one validity restriction as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 9, Wong discloses the method according to claim 5. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle. However, England discloses wherein the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle. (see England col. 8,

lines 26-28; col. 9, lines 4-10: internal software identity register (validity restriction); uniquely determines the OS; col. 8, line 66 - col. 9, line 3: trusted third party to digitally sign all components)

It would have been obvious to one of ordinary skill in the art to modify Wong for restriction to a particular control unit designated by an identification number as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 10, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. However, England discloses wherein the software signature certificate is checked for integrity according to a public-key method, using a public key of the trust center. (see England col. 8, line 66 - col. 9, lines 3: all components digitally signed by a trusted third party; col. 8, lines 7-12: public/private usage for manufacturer)

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, and checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider

without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 11, Wong discloses the method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. However, England discloses wherein the signed software is checked for integrity according to a public key method, using the public key of the software signature site contained in the software signature certificate. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

It would have been obvious to one of ordinary skill in the art to modify Wong for checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 12, Wong discloses the method according to claim 5. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the clearing code site signature certificate is checked for integrity

according to a public key method, using a public key of the trust center. However, England discloses wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-12: public/private key pair usage; checked for validity)

It would have been obvious to one of ordinary skill in the art to modify Wong to check for integrity according to a public key method, using a public key of the trust center as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 13, Wong discloses the method according to claim 4. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8: control unit for vehicle) Wong does not specifically disclose the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate. However, England discloses wherein the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised; col. 8, lines 7-

12: public/private key pair usage; checked for validity)

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, and checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 14, Wong discloses the method according to claim 1, wherein the control unit is equipped with a sequence-controlled microprocessor that implements one of the above-described methods. (see Wong col. 2, lines 21-29: vehicle processor (microprocessor))

Regarding Claim 15, Wong discloses a control unit for a motor vehicle, which implements a method according to claim 1. (see Wong col. 2, lines 21-29; col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: control unit, vehicle)

Regarding Claim 16, Wong discloses a data processing system for a motor vehicle, which implements a method according to claim 1. (see Wong col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: computer, data processing system)

Regarding Claim 17, Wong discloses a computer program product sequence control of

a data processing system of a motor vehicle or motorcycle, which implements the method according to claim 1. (see Wong col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: computer, data processing system, vehicle)

Regarding Claim 18, Wong discloses a data carrier, comprising a computer program product according to claim 17. (see Wong col. 4, line 64 - col. 5, line 8; col. 7, lines 35-39: software (computer program product) implementation means)

Regarding Claim 19, Wong discloses a method of providing software for use by a control unit of a vehicle, said method comprising:

the control unit (see Wong col. 7, lines 32-38: control unit, vehicle)

Wong does not specifically disclose whereby storing certificates, receiving signed software, checking signed software.

However, England discloses:

a) storing, a software signature certificate; receiving, signed software; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

b) checking, whether the software signature certificate has been changed or manipulated; (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)

c) checking, whether the signed software has been changed or manipulated. (see England col. 11, lines 54-59: checks signature of a component before loading it;

if signature valid then component has not been compromised)

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, and checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Regarding Claim 20, Wong discloses the method of claim 19, further comprising:

the control unit (see Wong col. 7, lines 32-38: control unit, vehicle)

Wong does not specifically disclose whereby storing certificates and keys associated with certificates.

However, England discloses:

a) storing, a trust center certificate that includes a public key and a signature generated using a secret key of a trust center; (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU) and

b) storing, a clearing code site signature certificate that includes a second public key and a second signature, (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

c) wherein the software signature certificate includes a third public key and a third

signature. (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to CPU)

It would have been obvious to one of ordinary skill in the art to modify Wong for signing the software against falsification, and checking the signed software for integrity as taught by England. One of ordinary skill in the art would have been motivated to employ the teachings of England in order to protect the rights of the content provider without requiring additional hardware directed at securing downloaded content. (see England col. 3, lines 57-61)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
October 14, 2008